20.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月１５日

出願番号
Application Number: 特願２００４－００７６８３

[ST. 10/C]: ［ＪＰ２００４－００７６８３］

出願人
Applicant(s): 松下電器産業株式会社

２００５年　１月２８日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３００４０３４

【書類名】　特許願
【整理番号】　2048150075
【提出日】　平成16年 1月15日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　横田　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　森岡　幸一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　石原　秀志
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　館林　誠
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
機器内部に保持される機器固有の秘密情報を確認する方法であって、
　機器固有の秘密情報に付随するインデックス情報を出力するための命令を機器に送信する命令送信ステップと、
　前記命令の送信を受けて、前記機器内部に保持する前記インデックス情報を出力するインデックス情報出力ステップとを含むことを特徴とする確認方法。
【請求項２】
機器内部に保持される機器固有の秘密情報を確認する機能を有する機器であって、
　機器外部から送付される機器固有の秘密情報を確認するための命令コマンドを受け付ける受付手段と、
　前記機器固有の秘密情報に付随し、機器固有の秘密情報を一意に指し示すインデックス情報を保管するインデックス情報保管部と、
　前記機器固有の秘密情報を機器外部からはアクセスできないようにして保管する秘密情報保管部と、
　前記受付手段が前記命令コマンドを受け付けると、前記インデックス情報保管部に保管する前記インデックス情報を機器外部に出力する出力手段とを備えることを特徴とする機器。
【請求項３】
機器内部に保持される機器固有の秘密情報を確認する機能を有する機器であって、
　機器外部から送付される機器固有の秘密情報を確認するための命令コマンドを受け付ける受付手段と、
　前記機器固有の秘密情報に付随し、機器固有の秘密情報を一意に指し示すインデックス情報を保管するインデックス情報保管部と、
　前記インデックス情報を暗号化する暗号化手段と、
　前記機器固有の秘密情報を機器外部からはアクセスできないようにして保管する秘密情報保管部と、
　前記受付手段が前記命令コマンドを受け付けると、前記インデックス情報保管部に保管する前記インデックス情報を前記暗号化手段で暗号化して機器外部に出力する出力手段とを備えることを特徴とする機器。
【請求項４】
前記インデックス情報は、前記機器固有の秘密情報を識別するための識別データと前記識別データに所定の変換を施した結果のデータである認証データを含むことを特徴とする請求項２または請求項３に記載の機器。
【請求項５】
さらに前記機器は、外部から記録媒体を挿入するための記録媒体装着手段を有し、
　前記命令コマンドを含んだプログラムが記録された記録媒体を前記記録媒体装着手段に挿入されると、前記受付手段が前記記録媒体に記録された前記プログラムに含まれる前記命令コマンドを受け付けることを特徴とする請求項２から請求項４のいずれか１項に記載の機器。
【請求項６】
前記受付手段は、通信端子であることを特徴とする請求項２から請求項４のいずれか１項に記載の機器。
【請求項７】
前記受付手段は、前記機器の開発時に使用するデバッグ用端子であることを特徴とする請求項２から請求項４のいずれか１項に記載の機器。
【請求項８】
前記記録媒体には、一意な識別番号が記録され、
　前記受付手段は、前記記録媒体装着手段に挿入される記録媒体の識別番号がある一定の条件を満たすことを確認し、満たす場合に限り前記命令コマンドを受け付ける、命令実行

許可手段を含むことを特徴とする請求項５に記載の機器。
【請求項９】
機器内部に保持される機器固有の秘密情報を確認する機能を有する機器であって、
　前記機器固有の秘密情報に付随し、機器固有の秘密情報を一意に指し示すインデックス情報を表示する、インデックス情報表示手段を有することを特徴とする機器。
【請求項１０】
機器内部に保持される機器固有の秘密情報を確認する機能を有する機器であって、
　前記機器固有の秘密情報に付随するインデックス情報または前記インデックス情報を暗号化した暗号化インデックス情報を表示するインデックス情報表示手段を有することを特徴とする機器。

【書類名】明細書
【発明の名称】機器固有秘密情報を確認する手段を備えた機器及び機器固有秘密情報の確認方法
【技術分野】
【０００１】
本発明は、各機器に埋め込まれる機器固有の情報を確認する手段を備えた機器、及び、機器固有の情報を確認する方法に関する。
【背景技術】
【０００２】
ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）などの光ディスクやＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）メモリーカード、メモリースティックなどの半導体記録メディアなどの記録メディアに対するデジタルコンテンツ著作権保護方式では、コンテンツは暗号化されてメディアに記録されている。再生時には、再生機器に埋め込まれた鍵を用いて復号化され、再生される。機器を製造するメーカは、著作権保護技術の使用をライセンスするライセンサとの間でライセンス契約を締結した上で、ライセンサより機器の製造ライセンス許諾とともに上記コンテンツ復号化に必要となる鍵（デバイス鍵）を受ける。前記ライセンス契約には、機器を製造する際のセキュリティ実装規約（コンプライアンスルール、ロバストネスルール）が含まれており、受け取ったデバイス鍵をある一定のセキュリティ基準を満たす形で機器内部に実装することや、機器内で復号化した平文のコンテンツデータを汎用の外部インタフェースを介して機器の外部に出力することや、機器内のユーザアクセシブルバスに出力することをしてはならない、などの実装条件がライセンスを受けたメーカに強制化される。上記のようなデバイス鍵によるコンテンツ暗号化の仕組みと契約による実装規約の遵守によって、メディアに記録されるコンテンツがハードディスクや他の記録メディアへ不正コピーされることや、インターネットなどへ不正に流出することを阻止することができる。
【０００３】
しかしながら、上記のような仕組みだけでは、万一、メーカがデバイス鍵を機器に埋め込む際に施した保護実装が解除されて、デバイス鍵が暴露されてしまった場合の脅威には対抗することができない。即ち、デバイス鍵の暴露を行った解析者は、そのデバイス鍵を元に、暗号化コンテンツを復号化してハードディスクにコピーするような（つまり、前記セキュリティ実装規約を無視した）不正なコピーツールを作成して流布することが可能となるが、前記のコンテンツ暗号化の仕組みだけでは、このような解析者による不正行為を防ぐことができない。
【０００４】
そこで、多くの著作権保護方式では、上記のようなデバイス鍵暴露に対する対抗策として、鍵無効化の技術を導入している。鍵無効化の具体的な方法としては、例えば非特許文献１に開示されている方法がある。この鍵無効化方式では、各機器には機器固有のデバイス鍵が与えられる。また、各デバイス鍵にはデバイス鍵を識別するためのインデックス情報（以下、デバイス鍵インデックス情報と呼ぶ）が割り当てられており、デバイス鍵とともに各機器に与えられる。機器は暗号化されたコンテンツを前記デバイス鍵とそれに付随するデバイス鍵インデックス情報を元に復号化することが可能となる。この技術を用いると、万一あるデバイス鍵が暴露されたとしても、そのデバイス鍵を無効化することができ、無効化された以降に製造される記録メディアに書き込まれるコンテンツ、あるいは、無効化された以降に製造される記録済みメディア上コンテンツは、その無効化されたデバイス鍵では復号化できないようにできる。上記技術の詳細については、非特許文献１に記載されているので、ここではこれ以上の詳細説明はしない。以上のように、鍵の無効化技術では、機器ごとに異なるデバイス鍵を埋め込み、これによって暴露されたデバイス鍵を個別に無効化することができる。
【非特許文献１】奥秋清次、サントソバグス、太田和夫、「Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ　ＴｈｅｏｒｙとＳｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ　Ｍｅｔｈｏｄを融合したＨｙｂ

ｒｉｄ　Ｓｙｓｔｅｍの提案」、２００３年暗号と情報セキュリティシンポジウム予稿集、Ｖｏｌｕｍｅ　Ｉ、Ｐ．２２１－Ｐ．２２６、２００３年

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、鍵無効化技術においては機器ごとに個別のデバイス鍵を機器に埋め込む必要があり、また、契約条件からそれらのデバイス鍵を外部から読み取ることができないようにしなければならない。このことは、機器メーカにとっては非常に不都合である。なぜならば、動作不具合などによりエンドユーザが機器の修理依頼を受けた場合、不具合箇所の特定、特に、不具合が復号か処理部で生じているのかどうかを判別するためには、機器に埋め込まれているデバイス鍵の内容を知る必要があるからである。例えば、いくつかのデバイス鍵の無効化が実際に行われた状況下で、修理依頼を受けた機器が無効化されたデバイス鍵が埋め込まれた機器なのかどうかを判別するためには、デバイス鍵の内容を知る必要がある。

【０００６】

一方、別の観点からも以下のような問題がある。デバイス鍵は機器一台ごとに異なる鍵を使うことが必須であり、著作権保護技術のライセンサは、ライセンシである機器メーカが契約を無視して、複数の機器に同じデバイス鍵を埋め込むような不正行為をしていないかをいつでも確認できる必要がある。このような必要性に対して、現状では、デバイス鍵は機器から読み取ることができないように実装されているために知ることができず、埋め込まれているデバイス鍵の識別は非常に困難である。

【０００７】

本発明は、前記の課題を解決するもので、機器に個別の鍵が外部から読み取りできないように実装されている場合でも、機器に埋め込まれている鍵がどれであるかを判別することが可能な機器固有情報の確認方法を提供することを目的とする。

【課題を解決するための手段】

【０００８】

前記従来の課題を解決するために、本発明の機器に埋め込まれた機器固有情報を確認する手段を備える機器は、機器外部から送付される機器固有の秘密情報を確認するための命令コマンドを受け付ける受付手段と、前記機器固有の秘密情報に付随し、機器固有の秘密情報を一意に指し示すインデックス情報を保管するインデックス情報保管部とを有し、前記受付手段が前記命令コマンドを受け付けると、前記インデックス情報保管部に保管する前記インデックス情報を機器外部に出力する出力手段とを備えることを特徴とする。

【０００９】

本構成によって、本発明の機器では、製品として出荷された後でも、機器内にどの機器固有の秘密情報が埋め込まれているのかを確認することが可能となる。

【発明の効果】

【００１０】

本発明の機器固有情報の確認方法によれば、機器固有のデバイス鍵を外部からは読み取りできないように実装された後でも、機器にどのようなデバイス鍵を埋め込んでいるのかを確認することが可能となる。

【発明を実施するための最良の形態】

【００１１】

以下本発明の実施の形態について、図面を参照しながら説明する。

【００１２】

本実施の形態の機器１では、以下の第１～第４の構成例のうちいずれによってでも、機器内部のデバイス鍵を確認することが可能である。

【００１３】

（第１の構成例）

図１は、本発明の機器固有情報の確認方法を用いて機器１に埋め込まれているデバイス

鍵を確認するための第１の構成例である。

【００１４】

本構成例では、機器固有のデバイス鍵とそれに付随するデバイス鍵インデックス情報が埋め込まれている機器１と、機器に埋め込まれたデバイス鍵の内容を表示装置３に表示するためのプログラムを格納した光ディスク２と、機器１が出力するビデオデータを画面に表示するための表示装置３とからなる。機器１と表示装置３は、ビデオ入出力のためのインタフェースを具備している。ここで光ディスク２としては、ＤＶＤやＢＤ（Ｂｌｕ－ｒａｙ）ディスクやＣＤなど、機器１としては、ＤＶＤプレーヤ、ＤＶＤレコーダ、ＢＤレコーダなど、ビデオ入出力のためのインタフェースとしては、ＲＧＢ端子、ビデオ端子、Ｓ端子、Ｄ端子などが想定され、それぞれの端子用に応じた接続ケーブルによって機器１と表示装置３は接続されている。

【００１５】

機器１に埋め込まれているデバイス鍵情報を取得する方法は以下の通りである。まず、機器１に光ディスク２を挿入する。次に、機器１は挿入された光ディスク２に記録されているプログラムを読み取り、そのプログラムに従って、デバイス鍵インデックス情報を出力する。出力されたデバイス鍵インデックス情報は接続ケーブルを介して表示装置３に入力され、表示装置３は、デバイス鍵インデックス情報を示す映像を画面に表示する。インデックス情報から、どのデバイス鍵が埋め込まれているかを知ることができる。光ディスク２が挿入されてからデバイス鍵インデックス情報を出力するまでの機器１内部の詳細動作については後で説明する。本構成例では、機器１で既に実装されている光ディスク読み取り手段と、外部への映像出力インタフェースを利用するため、デバイス鍵インデックス情報を出力するためのプログラムを機器１に追加するだけで済み、機能追加のためのコストが少なくて済む。

【００１６】

（第２の構成例）

本実施の形態では、第１の構成例に加えて、以下の第２の構成例によってもデバイス鍵の情報を得ることができる。

【００１７】

図２は、本発明の機器固有情報の確認方法を用いて機器１に埋め込まれているデバイス鍵を確認するための第２の構成例である。

【００１８】

本構成例では、第１の構成例と同じ機器１と、機器１内部のプログラムなどをデバッグするためのデバッグ装置４１とデバッグ装置４１からの出力を受けて画面表示を行う表示装置４２と、デバッグ装置４１の操作者から受けた入力をデバッグ装置４１へ入力するための入力装置４３とからなる。デバッグ装置４１は、機器１の開発において使用するデバッグ装置と同一のものである。機器１とデバッグ装置４１は、例えばＪＴＡＧ（Ｊｏｉｎｔ　Ｔｅｓｔ　Ａｃｔｉｏｎ　Ｇｒｏｕｐ）のようなデバッグ端子を具備しており、これらの端子間はＪＴＡＧケーブルなどデバッグ装置接続用の端子に対応する接続ケーブルによって接続されている。また、デバッグ装置４１と表示装置４２、及び４１と入力装置４３は用いるデバッグ端子に対応した接続ケーブルで接続されている。

【００１９】

機器１に埋め込まれているデバイス鍵情報を取得する手順は以下の通りである。まず、機器１に接続された状態でデバッグ装置４１を起動する。次に、操作者は入力装置４３を用いて、機器１内部のデバイス鍵情報を表示するための命令をデバッグ装置４１に入力する。命令を受けたデバッグ装置４１は、機器１に対してデバイス鍵インデックス情報を出力するための所定の命令コードを送信する。前記命令コードを受け取った機器１は、機器１内部に保持しているデバイス鍵インデックス情報をデバッグ装置４１に送信する。そして、デバッグ装置４１は、受け取ったデバイス鍵インデックス情報を表示装置４２の画面に表示可能なデータ形式に変換した上で、表示装置４２に送信する。表示装置４２は受け取った表示用データを元に、デバイス鍵インデックス情報を画面に表示する。命令コード

を受け取ってからデバイス鍵インデックス情報をデバッグ装置４１に送信するまでの機器１内部の詳細動作については後で説明する。

【００２０】

本構成例では、機器開発用のデバッグ用インタフェースをそのまま利用できるため、デバイス鍵インデックス情報取得のための専用のインタフェースを設けずに済むというメリットがある。また、デバッグ用のインタフェースを利用することで、機器開発用のデバッガ端末、デバッグ環境を持たない一般ユーザなどが不正にデバイス鍵インデックス情報を閲覧することを防止できる。

【００２１】

（第３の構成例）

さらに本実施の形態では、以下の第３の構成例によってもデバイス鍵の情報を得ることができる。

【００２２】

図３は、本発明の機器固有情報の確認方法を用いて機器１に埋め込まれているデバイス鍵を確認するための第３の構成例である。

【００２３】

本構成例では、第１、第２の構成例と同じ機器１及び表示装置３と、機器１と、及び、サーバ６との間でやり取りされるデータ伝送を行うためのネットワーク５と、機器１に内部のデバイス鍵情報を出力するための命令コマンドを送信するサーバ６とからなる。機器１にはネットワーク５に接続するためのインタフェースを具備しており、具体的にはＬＡＮ端子などが想定される。

【００２４】

機器１に埋め込まれているデバイス鍵情報を取得する方法は以下の通りである。まず、操作者が、機器１に所定の操作を行って機器メンテナンス用メニュを表示装置３に表示させる。これは、例えば機器１の本体にメンテナンスモードに移行するための特別なスイッチを設け、それを押すことによって移行するようにすればよい。操作者は表示メニュの中から、「デバイス鍵情報の取得処理の実行」のメニュを選択する。このとき、操作者によるメニュ選択操作は、機器１の本体に設置されている操作用ボタンを用いて行うようにしてもよいし、機器１に付属のリモートコントローラーによって行うようにしてもよい。上記メニュの選択後、機器１は、ネットワーク５を介してサーバ６に接続要求を送信する。上記要求を受けたサーバ６は、機器１の操作者が要求された処理（即ち、デバイス鍵情報の表示処理）を実行する権限のあるものであるかをパスワード認証によって行う。具体的には、サーバ６に予め、上記権限のある操作者のユーザ名とパスワードを登録しておき、操作者が登録されたユーザ名とパスワードを正しく入力するかによって認証を行う。上記認証によって、操作者の確認ができた後、サーバ６は、デバイス鍵情報表示を行うための命令コマンドを、ネットワーク５を介して機器１に送信する。そして、上記命令コマンドを受け取った機器１は、デバイス鍵インデックス情報を表示装置３に入力し、表示装置３はその情報を画面に表示する。上記命令コマンドを受け取ってからデバイス鍵インデックス情報を表示装置３に入力するまでの、機器１内部の詳細動作については後で説明する。

【００２５】

本構成例の場合、例えばＥＰＧ情報の更新や録画予約をネットワーク経由で行うための通信インタフェースを有するＤＶＤレコーダ機器などの場合には、デバイス鍵インデックス情報取得のための専用のインタフェースを設けずに済むというメリットがある。

【００２６】

また、サーバ６は、操作者にデバイス鍵インデックスを閲覧する権限があるかどうかを認証するので、権限のない操作者が不正にデバイス鍵インデックスを閲覧することを防止することができる。

【００２７】

（第４の構成例）

さらに本実施の形態では、以下の第４の構成例によってもデバイス鍵の情報を得ること

ができる。

【００２８】

図４は、本発明の機器固有情報の確認方法を用いて機器１に埋め込まれているデバイス鍵を確認するための第４の構成例である。

【００２９】

本構成例では、第１、第２、第３の構成例と同じ機器と、コンピュータ端末７１との間でやり取りされるデータ伝送を行うためのネットワーク５と、コンピュータ端末７１から出力される表示情報を画面に表示する表示端末７２と、コンピュータ端末７１にデータ入力を行うための入力端末７３とからなる。機器１及びコンピュータ端末７１にはネットワーク５に接続するためのインタフェースを具備しており、具体的にはＬＡＮ端子などが想定される。また、コンピュータ端末７１には、機器１内部のデバイス鍵の情報をモニターするためのプログラムがインストールされている。

【００３０】

機器１に埋め込まれているデバイス鍵情報を取得する方法は以下の通りである。まず、機器１とコンピュータ端末７１とがネットワーク５を介して接続された状態でコンピュータ端末７１にてデバイス鍵をモニターするためのプログラムを起動する。次に、コンピュータ端末７１の操作者は入力端末７３を用いて、デバイス鍵情報を表示するための命令をコンピュータ端末７１に入力する。命令を受けたコンピュータ端末７１はデバイス鍵インデックス情報を出力するための命令コードを、ネットワーク５を介して機器１に送信する。前記命令コードを受け取った機器１は、デバイス鍵インデックス情報をコンピュータ端末７１に送信する。そして、コンピュータ端末７１は、受け取ったインデックス情報を画面に表示するためのデータ形式に変換した後、表示端末７２に送信する。表示端末７２は受け取ったデータを元に、機器１のデバイス鍵インデックス情報を画面に表示する。コンピュータ端末７１から命令コードを受け取ってからコンピュータ端末７１にデバイス鍵インデックス情報を送信するまでの間の機器１内部の詳細動作については後で説明する。

【００３１】

本構成例の場合、例えばＥＰＧ情報の更新や録画予約をネットワーク経由で行うための通信インタフェースを有するＤＶＤレコーダ機器などの場合には、デバイス鍵インデックス情報取得のための専用のインタフェースを設けずに済むというメリットがある。

【００３２】

（機器１の内部構成と動作）

図５は本実施の形態に係る機器１の内部構成を示すブロック図である。

【００３３】

機器１は、各処理部やインタフェースの入出力及び各記憶部の読み出し／書き込みを制御するためのメイン処理部１０と、機器１内部処理データを表示装置３が画面表示するためのデータ形式に変換を行う映像処理部１１と、前記画面表示用データを表示装置３に出力する映像出力部１２と、デバッグ装置４１とのデータ入出力インタフェースであるデバッグ用外部Ｉ／Ｆ１３と、ＬＡＮなどの外部ネットワークに接続するための通信インタフェースである通信Ｉ／Ｆ１４と、機器１に挿入された光ディスクに記録されたデータを読み取りや光ディスクへのデータ書き込みを行うディスク読み取り部１５と、コンテンツ再生などの際に必要となる暗号処理を行う暗号処理部１７と、プログラムや機器１内部の処理データを一時的に格納するためのＲＡＭ１８と、機器に埋め込まれているデバイス鍵に付随するデバイス鍵インデックス情報を記憶するデバイスＩＤ記憶部１９と、デバイス鍵を記憶するデバイス鍵記憶部１１０と、機器１内部で実行するためのプログラムを記憶するプログラム記憶部１１１と、各モジュール間のデータ転送を行うデータバス１６とからなる。映像出力部１２としては、ＲＧＢ端子、ビデオ端子、Ｓ端子、Ｄ端子などが想定され、デバッグ用外部Ｉ／Ｆ１３としては、ＪＴＡＧ端子などが想定され、通信Ｉ／Ｆ１４としては、ＬＡＮ端子などが想定される。

【００３４】

デバイス鍵インデックス情報及びデバイス鍵は、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉ

ｏｎ　Ｓｔａｎｄａｒｄ）暗号のような所定の暗号方式によって暗号化されてそれぞれデバイスＩＤ記憶部１９及びデバイス鍵記憶部１１０に記憶されており、暗号化に使用した鍵（マスター鍵）は暗号処理部１７内部に外部から読み出しができないようにして記憶されている。プログラム記憶部１１１は、機器１内部の処理を行うためのプログラムが格納されている。ここに記憶されているプログラムには、外部からの命令コマンドに応じてデバイス鍵インデックス情報を外部に出力するための処理を記述するプログラムも含まれている。また、これらのプログラムはデータ圧縮されてプログラム記憶部１１１に記録されており、機器１の電源オン時にデータ展開されて、ＲＡＭ１８に転送される。

【００３５】

以下、第１から第５の構成例のそれぞれの場合について、機器１の内部処理について説明する。

【００３６】

（第１の構成例の場合）

図１及び図５を用いて、第１の構成例において、機器１がデバイス鍵インデックス情報を外部に出力する際の処理について説明する。

【００３７】

デバイス鍵インデックス情報を表示するためのプログラムが格納された光ディスク２が機器１のディスク挿入口に挿入された後、ディスク読み取り部１５は、光ディスク２に書き込まれているプログラムデータを読み取る。読み取られたプログラムデータは、データバス１６を介してメイン処理部１０に転送される。メイン処理部１０は、プログラムデータに含まれるデバイス鍵インデックス情報を出力するためのコマンドを読み取り、ＲＡＭ１８に記録されているデバイス鍵インデックス情報を外部に出力するための処理を記述するプログラムに従って以下の処理を行う。

【００３８】

まず、デバイスＩＤ記憶部１９に記憶している暗号化デバイスインデックス情報を読み取って暗号処理部１７に入力する。そして、暗号処理部１７にて、暗号化デバイスインデックス情報を復号化する。さらに、復号化されたデバイスインデックス情報を映像処理部１１で映像表示装置３によって表示可能なデータ形式に変換して、映像出力部１２を介して表示装置３に出力する。

【００３９】

（第２の構成例の場合）

次に図２及び図５を用いて、第２の構成例において、機器１がデバイス鍵インデックス情報を外部に出力する際の処理について説明する。

【００４０】

デバイス鍵インデックス情報を表示するためのコマンドがデバッグ用外部Ｉ／Ｆ１３及びデータバス１６を介してメイン処理部１０に入力される。メイン処理部１０は、前記コマンド入力を受けて、ＲＡＭ１８に記録されているデバイス鍵インデックス情報を外部に出力するための処理を記述するプログラムに従って第１の構成例の場合と同様の処理を行い、復号化デバイス鍵インデックス情報を算出する。そして、それをデバッグ用外部Ｉ／Ｆ１３を介してデバッグ装置４１に出力する。

【００４１】

（第３の構成例の場合）

次に図３及び図５を用いて、第３の構成例において、機器１がデバイス鍵インデックス情報を外部に出力する際の処理について説明する。

【００４２】

デバイス鍵インデックス情報を表示するためのコマンドが通信Ｉ／Ｆ１４及びデータバス１６を介してメイン処理部１０に入力される。メイン処理部１０は、前記コマンド入力を受けて、ＲＡＭ１８に記録されているデバイス鍵インデックス情報を外部に出力するための処理を記述するプログラムに従って第１、第２の構成例の場合と同様の処理を行い、復号化デバイス鍵インデックス情報を算出する。そして、それを映像処理部１１にて表示

装置３の画面に表示可能なデータ形式に変換し、映像出力部１２を介して表示装置３に出力する。

【００４３】

（第４の構成例の場合）

次に図４及び図５を用いて、第４の構成例において、機器１がデバイス鍵インデックス情報を外部に出力する際の処理について説明する。

【００４４】

デバイス鍵インデックス情報を表示するためのコマンドが通信Ｉ／Ｆ１４及びデータバス１６を介してメイン処理部１０に入力される。メイン処理部１０は、前記コマンド入力を受けて、ＲＡＭ１８に記録されているデバイス鍵インデックス情報を外部に出力するための処理を記述するプログラムに従って第１の構成例の場合と同様の処理を行い、復号化デバイス鍵インデックス情報を算出する。そして、それを通信Ｉ／Ｆ１４を介してデバイス鍵の情報モニターすることが可能なプログラムがインストールされたコンピュータ端末７１に出力する。

【００４５】

なお、本実施の形態では、デバイスインデックス情報を暗号化してデバイス鍵記憶部１１０に記憶しているが、これは暗号化せずにそのまま記憶してもよい。その場合には、デバイス鍵インデックス情報を外部に出力際には、デバイス鍵記憶部１１０から読み取ったデータをそのまま外部に出力すればよい。

【００４６】

また、本実施の形態では、暗号化デバイス鍵インデックス情報を暗号処理部１７にて復号化した後、外部に出力しているが、暗号化デバイス鍵情報をそのまま外部に出力しても良い。この場合には、暗号処理部１７には、暗号化デバイス鍵インデックス情報を復号化するための鍵が記憶されていない。機器１から上記データの入力を受けた装置側に復号化のための鍵が記憶されており、暗号化デバイス鍵インデックス情報を復号化することでデバイス鍵インデックス情報を求めるようにするか、暗号化されたままのデバイス鍵インデックス情報をそのまま表示させるようにしてもよい。あるいは、暗号処理部１７で復号化したデバイス鍵インデックス情報をさらに別の鍵で暗号化したものを表示させるようにしてもよい。さらに、前記暗号化デバイス鍵インデックス情報を復号化するための鍵は、各機器製造メーカが秘密に保持して、メーカしかデバイス鍵インデックス情報を知ることができないようにしてもよい。これによって、その機器を製造したメーカのみがデバイス鍵インデックス情報を知ることができるようになる。

【００４７】

また、本実施の形態の第１の構成例では、光ディスクを機器１に挿入する構成になっているが、これは、ＳＤメモリーカードやメモリースティックなどの半導体記録メディアやＩＣカードであってもよい。

【００４８】

また、本実施の形態の第１の構成例では一般ユーザが、自らデバイス鍵インデックス情報表示プログラムを格納した光ディスクを作成して機器内部のデバイス鍵インデックス情報を閲覧することを防ぐために、以下のような仕組みを追加してもよい。まず、光ディスクにはディスクごとにユニークなＩＤをディスク製造時にディスクのＲＯＭ領域に書き込んでおく。例えば、ＤＶＤの場合ＢＣＡ（Ｂｕｒｓｔ　Ｃｕｔｔｉｎｇ　Ａｒｅａ）にＩＤを書き込めばよい。そして、デバイス鍵インデックス情報を表示するための命令コマンドは、特定のＩＤをもつディスクが挿入された場合に限り、機器が実行するようにする。前記の特定のＩＤを持つ光ディスクは、市販されず、メンテナンス用ディスクとして、機器開発メーカのみが入手可能とする。これにより、一般ユーザがたとえデバイス鍵インデックス情報を表示するためのプログラムを作成できるとしても、上記メンテナンス用ディスクは入手できないので、機器内部のデバイス鍵インデックス情報は閲覧できない。

【００４９】

なお、本実施の形態では、第１、第２、第３、第４の構成例の全てを用いた構成として

いるが、これらのうち１つだけを用いた構成であってもよい。

【００５０】

さらに著作権保護技術のライセンサがライセンシである機器メーカが機器一台ごとに異なるデバイス鍵を正しく埋め込んでいるかを確認する目的で本発明の構成を適用する場合には、既に述べたようなデバイス鍵インデックス情報を外部に出力するためのコマンドを機器に実装することを契約などにより強制化すればよいが、以下のような問題が存在する。即ち、前記のコマンド自体は実装するが、そのコマンドによって出力するデバイス鍵インデックス情報は、実際に埋め込まれているものとは異なるものにするという不正である。具体的には、同じデバイス鍵及びデバイス鍵インデックス情報が複数の機器に埋め込まれているが、それぞれの機器では上記コマンドに応じて、それぞれの機器で異なる偽のデバイス鍵インデックス情報を出力することでライセンサには、異なるデバイス鍵が埋め込まれているように思わせることが可能となってしまう。この不正は以下のようにすれば防止できる。デバイス鍵インデックス情報をＤＩとしたとき、それに対してライセンサのみが知っている秘密の変換Ｆを施して、チェック情報Ｐ＝Ｆ（ＤＩ）を求める。Ｆとしては、例えば、鍵をライセンサのみの秘密とした秘密鍵暗号方式の暗号化処理が利用できる。ライセンサがライセンシである機器メーカにデバイス鍵を発行する際には、デバイス鍵、デバイス鍵インデックス情報に加えて前記のチェック情報Ｐを発行する。ライセンシには、デバイス鍵インデックス情報とチェック情報を結合して表示するためのコマンドを機器に実装することを契約などで強制化する。このようにすれば、ライセンシが架空のデバイス鍵インデックス情報を捏造しても、それに対応するチェック情報までを偽造することができなくなるので、前記のような偽のデバイス鍵インデックス情報を出力してもそれが捏造されたデバイスインデックス情報であることが、デバイス鍵インデックス情報ＤＩとチェック情報Ｐのペアの間にＰ＝Ｆ（ＤＩ）の関係が成り立つかをチェックすることで検出できる。また、前記の方法において、変換Ｆをライセンシも公開する場合には、上記のチェック情報Ｐあるいはデバイス鍵インデックスデータ ＤＩとチェック情報Ｐとを結合したデータをライセンサしか知りえない秘密の鍵で暗号化したデータをデバイス鍵とともにライセンシに発行し、デバイス鍵インデックス情報とともにこの暗号化データを出力するか、あるいは、デバイス鍵インデックス情報のかわりに前記の暗号化データを出力するコマンドを機器に実装することを強制化してもよい。この場合には、ライセンサは上記コマンドにより機器から前記暗号化データを取得して、ライセンサの秘密の鍵でこの暗号化データを復号化して得られたデータからデバイス鍵インデックス情報が捏造されたものでないかを確認できる。

【００５１】

また、デバイス鍵インデックス情報を表示装置などに表示させるのではなく、以下のようにしてもよい。図６（ｂ）は、図６（ａ）に示す機器１の上部カバーを外した時の図であり、筐体１ａと基盤１ｂとデバイス鍵インデックス情報表示部１ｃとからなる。デバイス鍵インデックス情報表示部１ｃは図６（ｃ）に示すように、機器１内部のデバイス鍵インデックス情報を１６進数で表示した数値が記載されている。これは、レーザー印刷などの印刷方法で直接印刷してもよいし、デバイス鍵インデックス情報を印刷した板をビスや粘着材あるいは溶接等の接着方法によって貼付してもよい。あるいは、デバイス鍵インデックス情報の印刷されたシールを貼付するのでもよい。記載される情報は具体的には、例えば非特許文献１に開示されている復号化情報Ｉｕを１６進数で表示した値を記載すればよい。機器１の上部カバーは特殊な形状のネジやビスなどで留めることによって、一般ユーザが外すことができないようにしてもよい。また、インデックス情報を表示する場所は、前記の場所に限らず機器１のインデックス情報であることが分かる箇所であればどこでもよい。

【産業上の利用可能性】

【００５２】

本発明にかかる機器は、外部からの命令コマンドを送信することで機器内部に埋め込まれている機器固有鍵の情報取得が可能となるという効果を有するので、例えば著作権保護

機能を有し、機器ごとにユニークな秘密情報が格納されている機器などに有用である。

【図面の簡単な説明】

【００５３】

【図１】本発明の実施形態に係る機器１と光ディスク２と表示装置３からなる第１の構成例の構成を示すブロック図

【図２】本発明の実施形態に係る機器１とデバッグ装置４１と表示装置４２とからなる第２の構成例を示すブロック図

【図３】本発明の実施形態に係る機器１とネットワーク５と表示装置３とサーバ６とからなる第３の構成例を示すブロック図

【図４】本発明の実施形態に係る機器１とネットワーク５とコンピュータ端末７１と表示端末７２と入力端末７３とからなる第４の構成例を示すブロック図

【図５】本発明の実施形態に係る機器１の構成例を示すブロック図

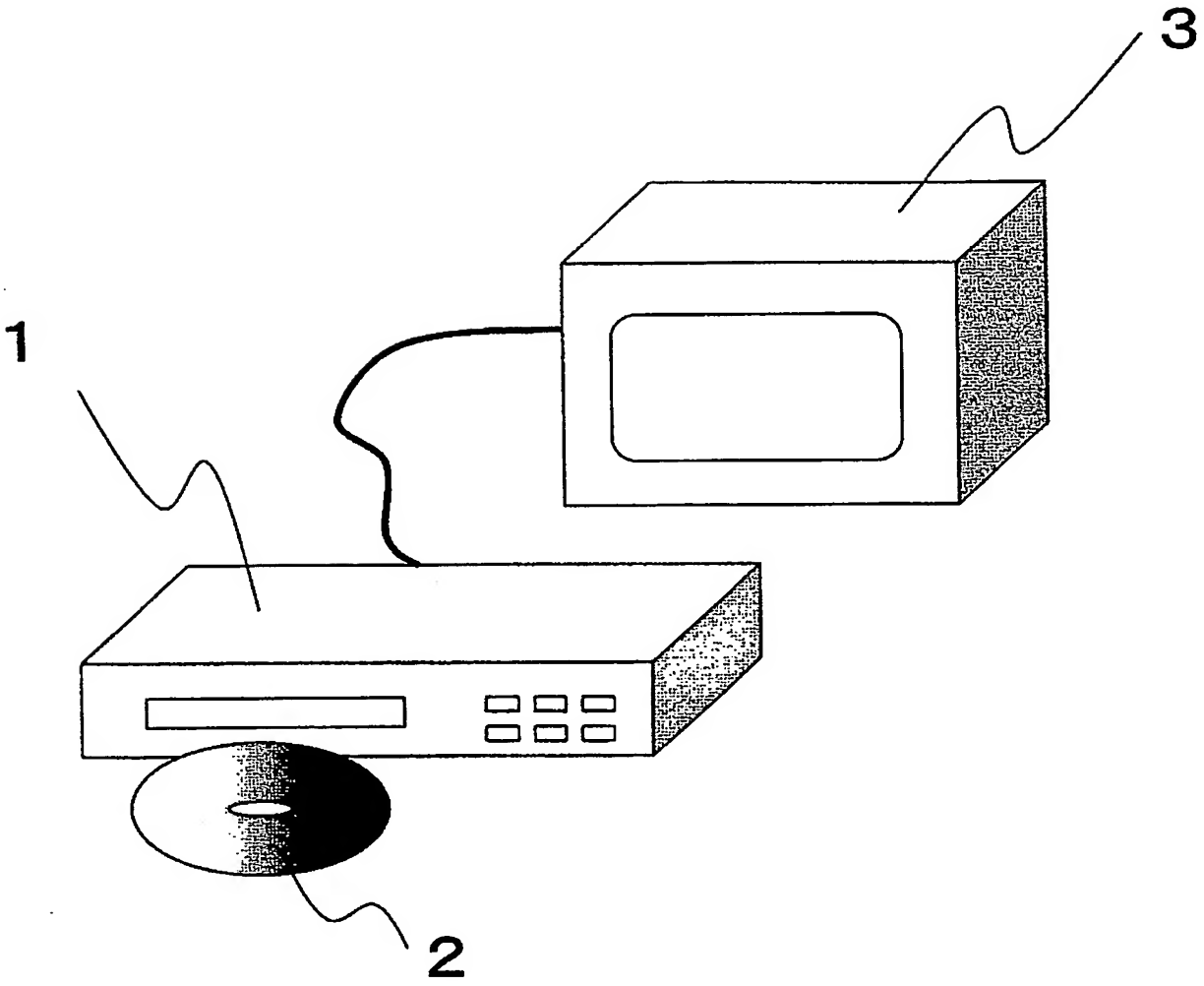
【図６】本発明の実施形態に係る機器１の一例を示すブロック図

【符号の説明】

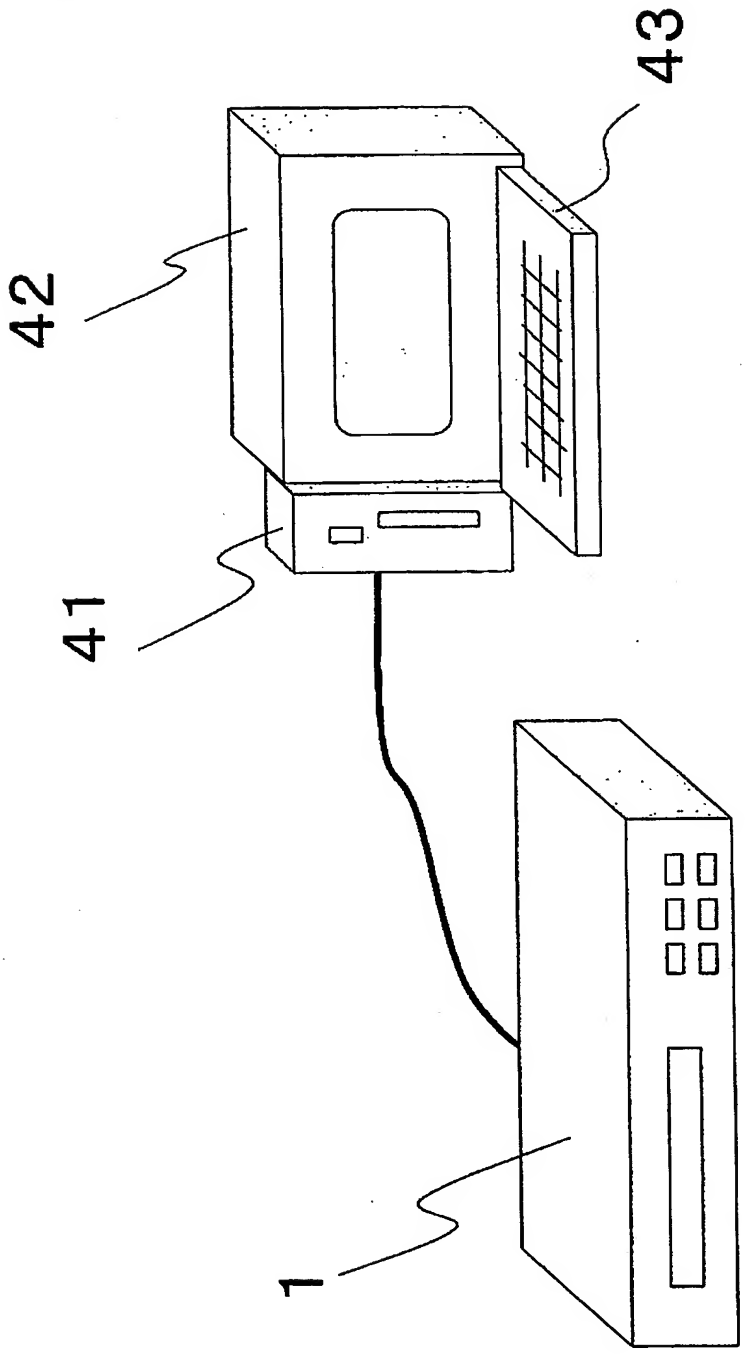
【００５４】

１　機器
２　光ディスク
３，４２　表示装置
５　ネットワーク
６　サーバ
１０　メイン処理部
１１　映像処理部
１２　映像出力部
１３　デバッグ用外部Ｉ／Ｆ
１４　通信Ｉ／Ｆ
１５　ディスク読み取り部
１６　データバス
１７　暗号処理部
１８　ＲＡＭ
１９　デバイスＩＤ記憶部
４１　デバッグ装置
４３　入力装置
７１　コンピュータ端末
７２　表示端末
７３　入力端末
１１０　デバイス鍵記憶部
１１１　プログラム記憶部

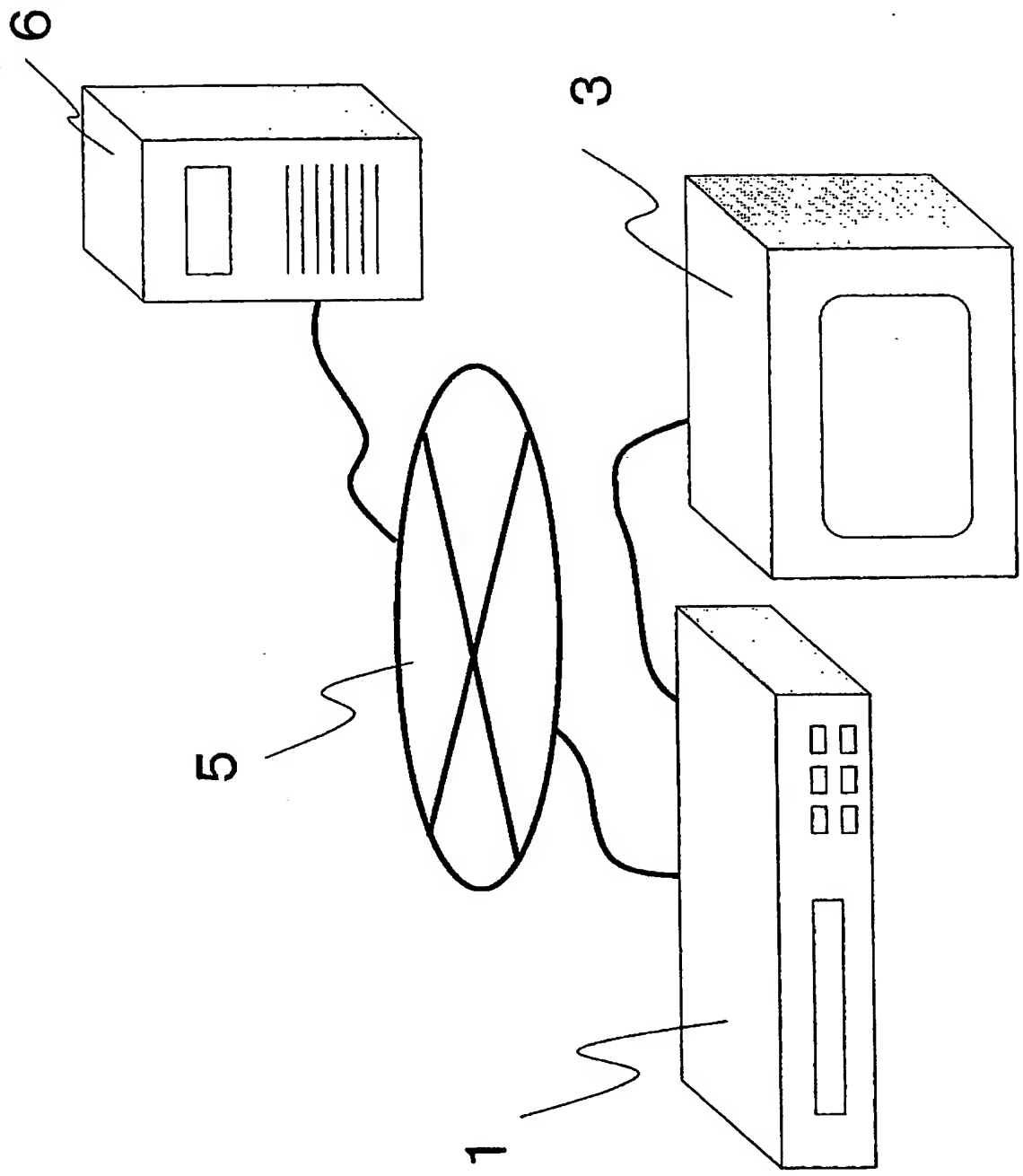
【書類名】図面
【図１】



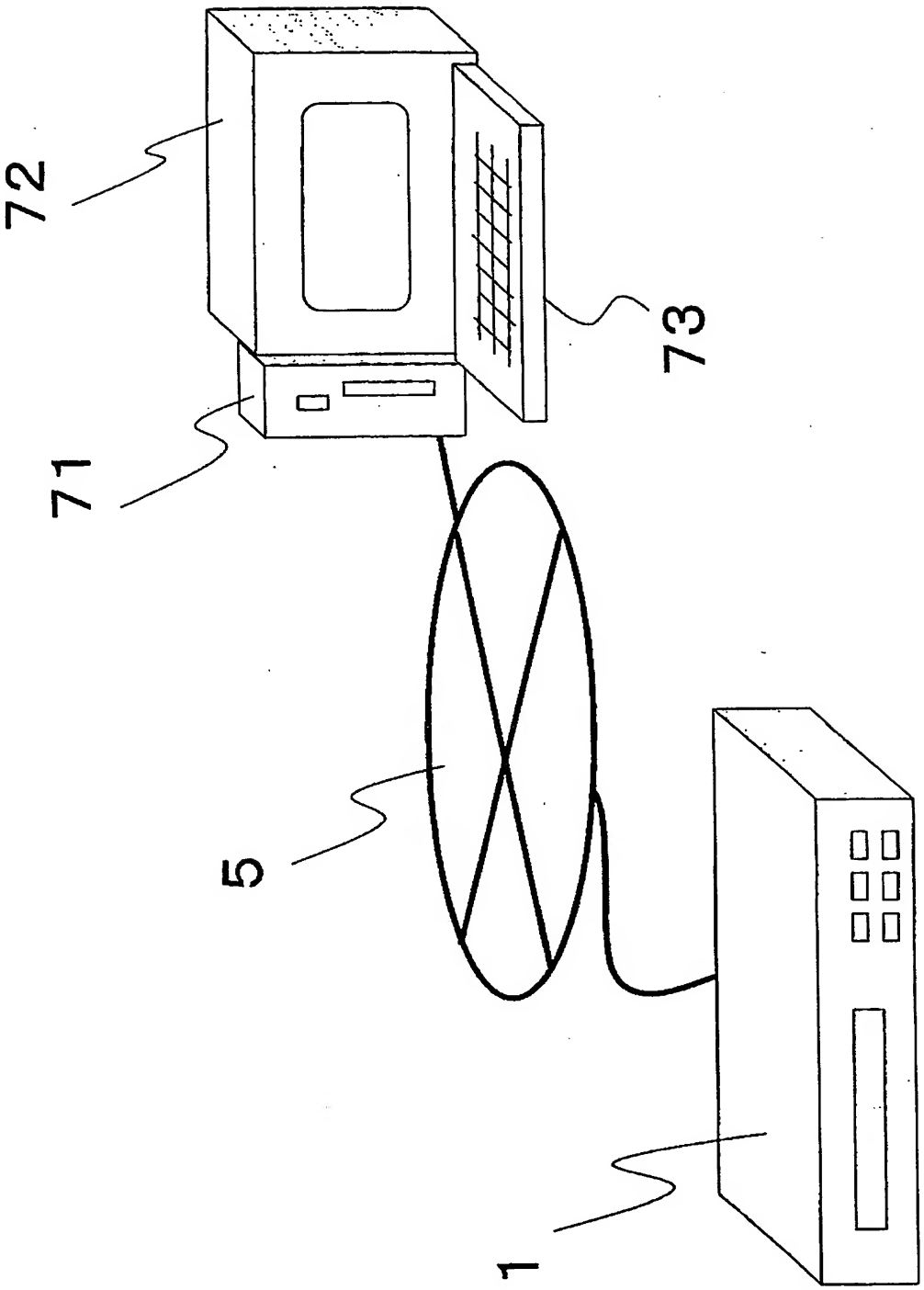
【図２】



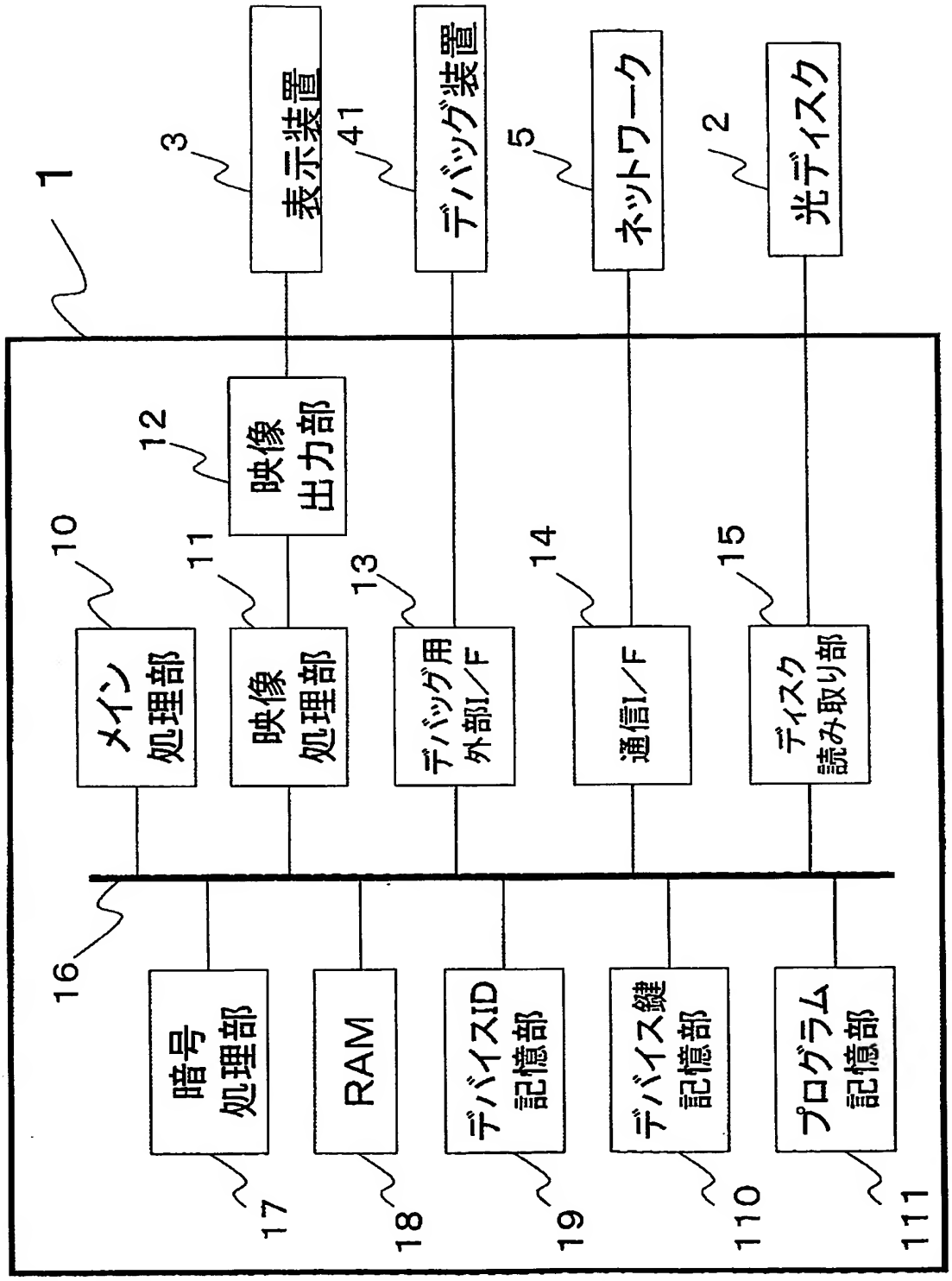
【図３】



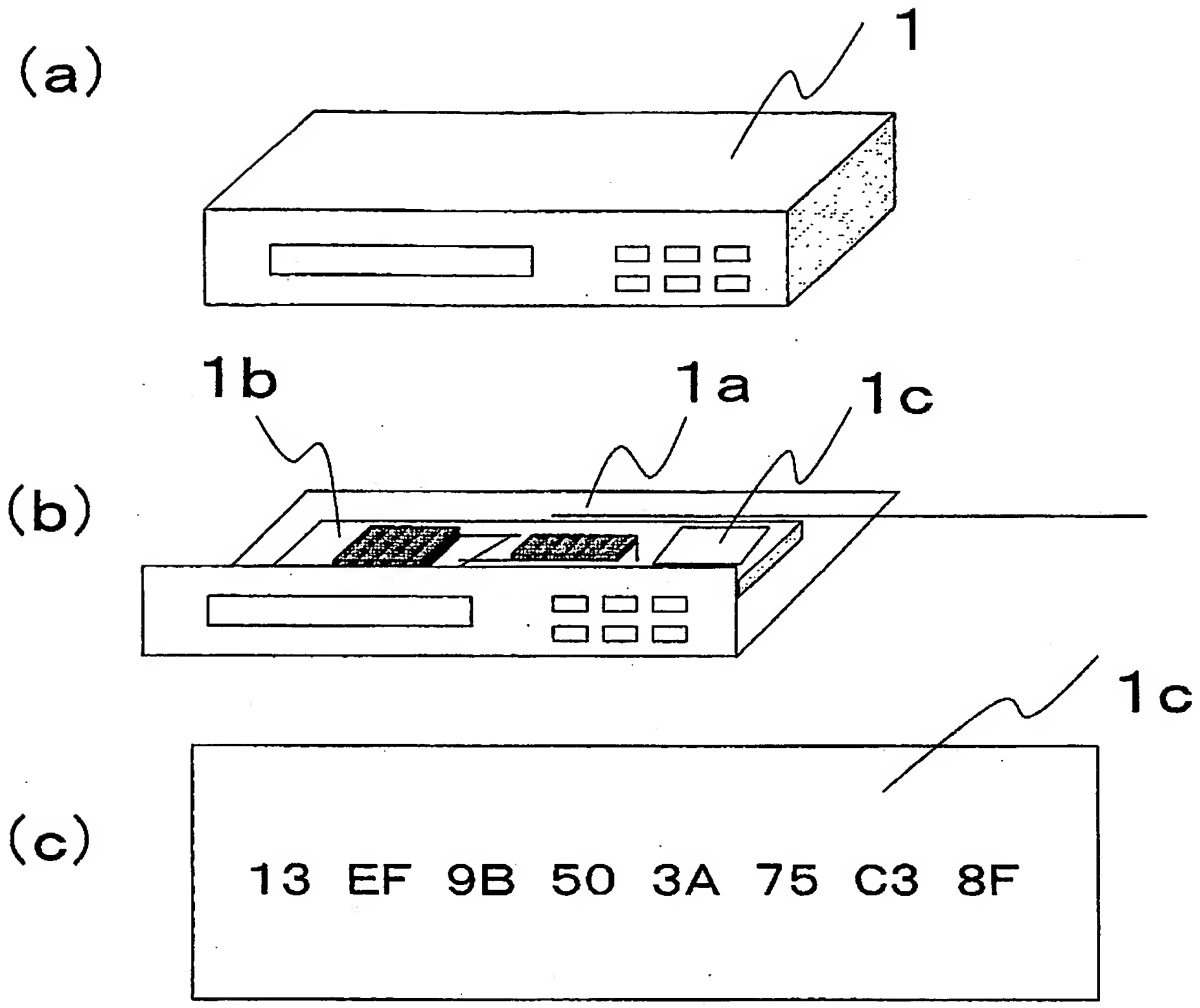
【図４】



【図５】


1
3
表示装置
41
デバッグ装置
5
ネットワーク
2
光ディスク
12
映像
出力部
10
メイン
処理部
11
映像
処理部
13
デバッグ用
外部I／F
14
通信I／F
15
ディスク
読み取り部
16
17
暗号
処理部
18
RAM
19
デバイスID
記憶部
110
デバイス鍵
記憶部
111
プログラム
記憶部

【図６】



【書類名】要約書
【要約】
【課題】機器内部に外部から参照できない状態で保持されている機器固有の秘密情報を確認する。
【解決手段】機器外部から送付される機器固有の秘密情報を確認するための命令コマンドを受け付ける受付手段と、前記機器固有の秘密情報に付随し、機器固有の秘密情報を一意に指し示すインデックス情報を保管するインデックス情報保管部とを有し、前記受付手段が前記命令コマンドを受け付けると、前記インデックス情報保管部に保管する前記インデックス情報を機器外部に出力する出力手段とを備える。
【選択図】図５

特願２００４－００７６８３

出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019479

International filing date: 20 December 2004 (20.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-007683
Filing date: 15 January 2004 (15.01.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse